Department of Homeland Security Daily Open Source Infrastructure Report for 23 June 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- TechWeb reports federal authorities have charged nine people with skimming bank account information from debit cards used by more than 100 people at restaurants in Southern California, resulting in the theft of more than $1 million. (See item 8)
- WUSA TV9 reports aviation authorities are investigating an incident in which someone may have trained a laser pointer at an airborne United Airlines plane en route to Dulles International Airport in Virginia. (See item 17)
- The Department of Homeland Security announced it has completed the congressionally mandated counterterrorism exercise TopOff 4 Command Post Exercise −− a multi−faceted effort to prevent and respond to a simulated terrorist attack using weapons of mass destruction. (See item 30)
- The Washington Post reports engineers hired by a Florida state agency are reporting that weaknesses in the dike around Lake Okeechobee pose a grave and imminent danger to the people and the environment of South Florida. (See item 39)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) −

http://www.esisac.com]

1. *June 22, Times Union (NY)* — **PSC targets utilities' response to storms.** The New York state Public Service Commission (PSC) wants electric utilities New York State Electric & Gas Corp. (NYSEG) and Con Edison to improve their communications practices with customers and elected officials in the wake of a severe windstorm that hit New York state in January. The storm left 60,000 customers of Consolidated Edison Inc. and 40,000 customers of NYSEG without power. Restoration efforts took as long as five days in the hardest−hit areas, and it followed a large storm that hit the state only a week earlier. The PSC said NYSEG must implement plans to improve communications with customers. The company must also expand its efforts to educate customers and public officials about the power−restoration process. Source: http://www.timesunion.com/AspStories/story.asp?storyID=49375 3

2. *June 21, Reuters* — **Earthquake shakes FirstEnergy Ohio Perry nuke.** A small earthquake shook FirstEnergy Corp.'s 1,235−megawatt Perry nuclear power station in Ohio Tuesday evening, June 20, but damaged no equipment and released no radiation. In a report to the U.S. Nuclear Regulatory Commission, the company said the quake occurred north−northwest of the plant site in North Perry in Lake County, about 35 miles northeast of Cleveland, at 4:11 p.m. EDT. The U.S. Geological Survey Website said the quake measured 3.4 on the Richter scale. Because of the seismic event, FirstEnergy declared an unusual event, which is the lowest of the NRC's four emergency classifications. The plant remained at full power. Source: http://today.reuters.com/stocks/QuoteCompanyNewsArticle.aspx?view=CN&storyID=2006−06−21T113224Z_01_N21301765_RTRIDST_0_UTILITIES−FIRSTENERGY−PERRY.XML&rpc=66

3. *June 21, Associated Press* — **Former Y−12 worker charged with taking files.** A former employee at the Y−12 National Security Complex in Oak Ridge, TN, has been charged with removing classified documents without authority, a misdemeanor. The U.S. Attorney's office has accused Everett Ashley Blauvelt Jr. of being "in possession of computer files and documents containing information classified at the Secret Restricted Data level, which he knowingly removed from the Y−12 complex without authority," according to an information filed in U.S. District Court on June 13. The incident happened in 2000. The information, which is similar to an indictment, said Blauvelt was going to keep the files on his personal computer at home. It was unclear what the files and documents contained, and no reason was given for the delay in charges. Y−12, a product of the World War II bomb−building Manhattan Project, continues to make components for every warhead in the country's nuclear arsenal. The complex is part of the Department of Energy's National Nuclear Security Administration. Source: http://www.knoxnews.com/kns/local_news/article/0,1406,KNS_34 7_4791905,00.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *June 22, SGV Tribune (CA)* — **Three injured in gas station pump fire.** Three people suffered minor injuries Wednesday, June 21, when fire broke out at a gas station in Azusa, CA, as a gas station employee attempted to repair a disconnected fueler hose. Intersections were blocked off, and a nearby mini−mart and restaurant were evacuated as a result.

Source: http://www.sgvtribune.com/news/ci_3966151

5. *June 22, Associated Press* — **Kentucky officials clearing debris from tanker explosion.** Officials said they hoped to reopen a western Kentucky road late Thursday afternoon, June 22, after a tanker loaded with 10,500 gallons of fuel turned over and exploded the night before in Paducah. Part of the Lowertown neighborhood was cleared out, with streets blocked, after gasoline and diesel fuel managed to leak in the storm sewer system. A nearby nursing home was also evacuated as a precaution.
Source: http://www.kentucky.com/mld/kentucky/news/local/14872958.htm

6. *June 22, Greeley Tribune (CO)* — **Clipped gas line in Colorado causes evacuation.** About 50 residents in Greeley, CO, were evacuated late Wednesday afternoon, June 21, after a construction worker clipped an underground gas line in the trailer community off 5th Street and 17th Avenue. Atmos Energy, formerly the Greeley Gas Co., repaired the gas line, and residents were able to return to their homes.
Source: http://www.greeleytrib.com/article/20060622/NEWS/106220092

[Return to top]

Defense Industrial Base Sector

7. *June 22, Government Accountability Office* — **GAO−06−274: Defense Logistics: Lack of a Synchronized Approach Between the Marine Corps and Army Affected the Timely Production and Installation of Marine Corps Truck Armor (Report).** The increasing threat of improvised explosive devices (IED) in Iraq has led to widespread interest by Congress and the public regarding the availability of critical force protection equipment. The Government Accountability Office (GAO) initiated a series of engagements under the Comptroller General's authority to address these concerns. In March 2006, GAO reported on factors that affected the production and installation of armor for the Army's medium and heavy trucks. This engagement examines issues affecting the production and installation of armor for the Marine Corps' medium and heavy trucks. The objectives were to (1) determine the extent to which truck armor was produced and installed to meet identified requirements, (2) identify what factors affected the time to provide truck armor, and (3) identify what actions the Marine Corps and the Department of Defense (DoD) have taken to improve the timely availability of truck armor. GAO is recommending that DoD (1) establish a process for sharing information on developing materiel solutions and (2) clarify the point at which the joint requirements process should be utilized. DoD concurred with the second recommendation but believes communication is sufficient to satisfy the first recommendation. GAO disagrees.
Highlights: http://www.gao.gov/highlights/d06274high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−274

[Return to top]

Banking and Finance Sector

8.

June 21, TechWeb — **Nine indicted in skimming scheme.** Federal authorities have charged nine with skimming bank account information from debit cards from more than 100 people at restaurants in Southern California. The information was used to steal money from the victims' bank accounts and purchase Postal money orders, a U.S. Postal Inspector said Wednesday, June 21. The United States Postal Inspection Service, IRS Criminal Investigation, and U.S. Immigration and Customs Enforcement believe the scheme resulted in the theft of more than $1 million. The nine were indicted by a federal grand jury in Santa Ana on charges that include conspiracy, bank fraud, and money laundering. Two defendants coordinated the scheme and instructed servers at three restaurants to steal account information from patrons' Wells Fargo Bank and Washington Mutual Bank debit cards. The two allegedly provided the restaurant servers with skimming devices capable of copying information contained on the debit cards' magnetic strips. They made their own Wells Fargo and Washington Mutual debit cards with the stolen information and asked banks to provide new personal identification numbers for the cards. After receiving new PIN numbers, the defendants allegedly used the cards to deposit counterfeit checks into the victims' accounts and withdraw cash and purchase postal orders. Source: http://www.techweb.com/article/printableArticle.jhtml;jsessionid=30H5SOUZIDSVYQSNDLRSKHSCJUNN2JVN?articleID=189600229&site_section=700028

9. *June 21, Computing (UK)* — **Bank of Scotland to cut waiting lines with RFID cards.** The Royal Bank of Scotland (RBS) has this week started testing RFID−equipped payment cards to reduce waiting lines in shops. The bank is working with MasterCard to test the contactless card payment system at its Edinburgh headquarters. A third of RBS's 3,000 staff have been issued with the cards, which allow them to pay for goods costing less than approximately US$10. Microscopic antennas fitted into the cards will allow employees to pay for goods by pressing the Maestro card onto a reader. Eight retail outlets, including Starbucks, Tesco, and a hairdresser's are participating in the pilot and have had their systems fitted with RFID reader pads. While payments using the contactless wipe method do not require pilot participants to enter a PIN security number, the bank will carry out random checks during the trial. MasterCard is carrying out a number of other tests with other banks across the world. Source: http://www.computing.co.uk/computing/news/2158771/rbs−trials−rfid−payment−cards

10. *June 21, Consumer Affairs* — **West Virginia closes advance fee scam.** West Virginia Attorney General Darrell McGraw says his office has successfully shut down a Canadian advanced fee loan scam operating under the name New Balance Express. McGraw said consumers complained that they were contacted by New Balance after submitting online loan applications. Some consumers applied for a loan directly on New Balance's Website. Others filed applications on a lender finder Website that apparently referred the loan to New Balance. New Balance claimed that it could get a loan for anyone, even if the consumer was a poor credit risk, as long as the advanced fees were paid before the loan proceeds were distributed. New Balance told consumers the fees were for advance payments on the loan, insurance, and collateral. Consumers were told that loan proceeds would be directly deposited to their checking accounts after the consumers wired the payments through Western Union. After wiring the advanced payments, consumers did not receive the loan proceeds. "When consumers submit loan applications, they are giving criminals their social security numbers, bank account numbers and other personal identifiable information that could result in them becoming a victim of identity

theft," McGraw warned.
Source: http://www.consumeraffairs.com/news04/2006/06/wv_advanced_fe e.html

11. *June 21, 1010 WINS (NY)* — **Crooks use explosives in attempt to rob ATM.** An attempt to set fire or blow up an ATM brought the bomb squad to a 24−hour bagel store in Chelsea, NY. A portion of the free−standing ATM was blown off outside 'New York City Bagel' store at the intersection of Sixth Avenue and 17th Street just after 12 am, Wednesday, June 21. Police say the suspects set fire to the ATM, in an apparent attempt to rob the cash inside. It was not clear if an improvised explosive device or a less technical lighter or blowtorch was used. The NYPD's bomb squad and crime scene responded to examine the ATM. Employees were inside during the explosion. Authorities have investigated several patterns of suspects stealing ATM machines from 24−hour businesses. According to police the thieves usually load the machines onto a truck and take them to another location, where they would open them with a blowtorch. It is not often that robbers attempt to detonate ATM's while still inside the businesses.
Source: http://1010wins.com/pages/49045.php

12. *June 21, U.S. Department of Agriculture* — **USDA notifies headquarters employees of possible personal information breach.** Agriculture Secretary Mike Johanns Wednesday, June 21, directed that notifications be sent to Washington, D.C. area employees of the U.S. Department of Agriculture (USDA) whose personal identity information might have been compromised when USDA computer systems were illegally accessed. Johanns was informed Wednesday of the possible breach during a briefing on the status of a forensic investigation into the incident. The intrusion took place during the first weekend in June. The personal identity information potentially accessed includes individual's names, social security numbers, and photos. Worksite information that is readily available to the public is also contained within the database. Approximately 26,000 current and former Washington, DC area USDA employees and contractors are potentially affected. USDA will provide free credit monitoring services for one year. The USDA Inspector General's Office is conducting a full investigation.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/06/0214.xml

[Return to top]

Transportation and Border Security Sector

13. *June 22, Associated Press* — **Department of Justice investigating alleged price−fixing by some airlines.** British and U.S. agencies are investigating alleged price−fixing by British Airways (BA) and other airlines on passenger fares and fuel surcharges, BA said Thursday, June 22. In a brief statement, BA said it was assisting the Office of Fair Trading and the U.S. Department of Justice with their investigations. Two other airlines −− Virgin Atlantic and American Airlines −− also said they were cooperating with the investigation. BA said Martin George, its commercial director, and Iain Burns, its head of communications, have been given leaves of absence during the probe. In February, more than a dozen airlines were drawn into an investigation by U.S. and European Union officials of suspected collusion in the air cargo industry to fix prices on surcharges for fuel, security, and insurance.
Source: http://www.usatoday.com/travel/news/2006−06−22−price−fixing− probe_x.htm

14. *June 22, Associated Press* — **FAA grounds Los Angeles County sheriff's drone plans.** The Los Angeles County sheriff's plan to use small, remote−controlled planes to track criminals and look for lost hikers has been temporarily grounded by federal officials worried about air safety. The Federal Aviation Administration (FAA) won't authorize the drones until it investigates a demonstration the sheriff's department conducted last week, FAA spokesperson Laura Brown said. She said agency officials told the sheriff's department it needed their authorization before flying the drones to ensure they don't interfere with other aircraft. The department could face disciplinary action over the demonstration. The five−pound, three−foot−long drones can beam video images 250 feet to deputies below. If they prove effective in tests, Sheriff Lee Baca plans to buy 20 drones for overhead surveillance, such as monitoring hostage situations and searching for fleeing suspects.
Source: http://hosted.ap.org/dynamic/stories/L/LOS_ANGELES_DRONE?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

15. *June 22, North Jersey Media* — **Amtrak trains again hit by power problems.** Power problems Wednesday, June 21, on Amtrak's Northeast Corridor lines stopped some trains between Newark and New York and delayed others. Amtrak officials have identified the source of the problem as a transmission line that carries high−voltage electricity around the rail system. Amtrak spokesperson Cliff Black said Wednesday's disruption does not appear to have anything in common with the low−voltage problems of June 2−3. Those failures temporarily shut down substations that convert commercial grade power to the frequency required by the railroad. Also, on May 25, an extensive failure stopped trains between Washington and New York, stranding thousands of travelers in tunnels under the Hudson River. Amtrak, which narrowly escaped bankruptcy in 2002, has a backlog of infrastructure needs worth $70 million, according to its 2007 request for federal funding. Among those needs is "essential rebuilding" of the Northeast Corridor's 100−year−old electric traction system. Amtrak has contracted with the North American Reliability Council, a regulatory organization, to investigate the cause of the May 25 outage. Some of the substations involved in the May 25 failure date to the 1930s.
Source: http://www.bergen.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk2OTUxNTkyJnlyaXJ5N2Y3MTdmN3ZxZWVFRXl5NA==

16. *June 22, South Florida Sun−Sentinel* — **Damaged freighter reported taking on water off Miami Beach.** A 184−foot−long freighter was reported taking on water off Miami Beach Wednesday, June 22, and the Coast Guard was working to get the vessel into port so that repairs could be made before it sinks. The Venezuelan−registered Sea Taxi may have developed the 120−gallon−a−minute leak by running aground as it left the Port of Miami on Wednesday, June 21, the Coast Guard said. A Coast Guard helicopter, rescue boat, and cutter responded to the call, and a crew from the cutter Sitkinak made temporary repairs to slow the amount of water the ship was taking on. The Coast Guard plans to allow the Sea Taxi to enter the Port of Miami during daylight using tugboats so that divers can fix the damage to the hull.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−622freighter,0,6158564.story?coll=sfla−home−headlines

17. *June 21, WUSA TV9 (DC)* — **Pilot reports laser pointed at plane.** Aviation authorities are investigating an incident in which someone may have trained a laser pointer at an airborne plane en route to Dulles International Airport in Virginia. The pilot of a United Air flight

reported someone shining a red light onto the left side of his craft about 9:45 p.m. EDT on Tuesday, June 20. The plane, an Airbus 320, was approaching Runway 19 at the time, but still about two miles from the airport and traveling at roughly 1,000 feet. The pilot of another flight, inbound to Dulles from Orlando, reported seeing someone o n the ground that may be responsible for the incident. The Metropolitan Washington Airports Authority is investigating and has referred information to the FBI. FAA research has shown that lasers shown into the cockpit can temporarily disorient or disable pilots during the critical stages of takeoff and landing.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=50293

18. *June 19, Department of Transportation* — **New grants for Ohio River Bridges project.** Federal Highway Administrator J. Richard Capka announced $5.2 million in new grants to move forward the Ohio River Bridges at an event to kick off a ramp relocation, part of the preliminary work necessary for the project to begin. “Today marks a significant first step toward a project that will relieve big city congestion, improve freight, and help the Louisville and southern Indiana economies,” Capka said. The new grants can be used on any aspect of the project, including the environmental process, design, and construction, according to Capka. The Ohio River Bridges project will improve congestion, safety, and mobility at a major mid−America crossroads of three interstates, I−65, I−64, and I−71. I−65 is a major north−south freight corridor between Mobile, AL. and Chicago, currently carrying more than 140,000 vehicles per day.
Source: http://www.dot.gov/affairs/fhwa0706.htm

[Return to top]

Postal and Shipping Sector

19. *June 22, Federal Times* — **USPS gains efficiency through contracting.** Though the U.S. Postal Service (USPS) has been ramping up its spending on outside contractors, some industry observers say it will have to outsource even more of its work if it aims to improve efficiency and remain competitive. For fiscal 2005 the Postal Service spent about $12 billion on contractors for goods and services, including fuel, according to David Hendel, attorney with Wickwire Gavin in Vienna, VA, and chairman of Wickwire Gavin’s Postal Industry Practice Group, which monitors Postal Service contractor spending. The agency’s top 10 suppliers provide air transportation, mail processing equipment, telecommunications, advertising, and other products and services. “The Postal Service is a $70 billion business, and a lot of its messages are still not getting out. FedEx and UPS are spending double and triple what they spend, ”said Gene Del Polito, of the Association for Postal Commerce. But before it spends more money on advertising, the Postal Service should determine exactly what kind of return it is generating from the money already spent, he said.
Source: http://federaltimes.com/index.php?S=1875434

[Return to top]

Agriculture Sector

20. *June 20, Associated Press* — **Finding chronic wasting disease in live animals.** A South Dakota State University scientist is doing research that could lead to a live animal test for chronic wasting disease (CWD). Alan Young, associate professor of veterinary science, said developing a culture system for CWD could lead to an early stage diagnosis. Current tests can be done only on dead animals' brains. "As far as progress goes, we're still a few years away from an actual diagnostic assay," he said.
Source: http://www.rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_4786892,00.html

21. *June 20, WALB (GA)* — **Soil−based disease threatens Georgia's watermelon crop.** With an increase in demand for seedless watermelons, farmers are working hard to keep up. But an old disease, deadly to the plant, has resurfaced and is threatening this crop. Fusarium wilt is a disease killing seedless watermelon crop in Georgia and all over the country. "When the watermelon roots grow in the soil, they come in contact with the fungus. The fungus attacks the root and begins to infect the root. It compromises the vascular system of the plant and cause the water intake to shut down which causes it to wilt," Plant Pathologist David Langston said. Since popping up around the turn of the twentieth century, fusarium wilt is one of the oldest and most destructive soil diseases. The industry has learned to breed resistant seeded watermelons so the wilt has not posed a major threat for quite some time. Watermelon eaters now prefer the seedless varieties. The only problem, they are not resistant to the disease. Industry officials are now charged with creating a wilt resistant variety of seedless watermelons. This process could take years.
Source: http://www.walb.com/Global/story.asp?S=5055983&nav=menu37_3

[Return to top]

Food Sector

22. *June 22, Dow Jones* — **U.S. Department of Agriculture to review seven beef plants.** The U.S. Department of Agriculture (USDA) will review production practices at seven U.S. beef plants in order to quell concerns raised by South Korea after its own inspectors complained of "deficiencies," USDA officials said. "We will review their corrective measures" after the U.S. beef plants make any changes to appease South Korea, one USDA official said. South Korea recently conducted a two−week audit of 37 U.S. beef processing plants to see first hand if they met the country's standards. South Korea has pledged to initially only reopen its market to boneless cuts. South Korea banned U.S. beef in December 2003 after the first case of mad cow disease was discovered in the U.S. Before the ban, the U.S. exported $815 million of beef to South Korea.
Source: http://www.cattlenetwork.com/content.asp?contentid=46820

23. *June 21, Agence France−Presse* — **Only a few Japanese businesses plan to serve U.S. beef.** Fewer than one in 10 Japanese restaurants and stores will immediately serve U.S. beef amid concerns over mad cow disease, after Tokyo lifted a ban, a poll shows. The Japanese government on Wednesday, June 21, ended a ban on imports of U.S. beef for second time in six months. Japan used to be the top overseas market for US beef. However, only 7.4 percent of restaurants and retailers said they would immediately resume U.S. beef sales when it returns to the market, which is expected in late July, the Nihon Keizai Shimbun said. Fifty percent said

they had no plans to resume beef imports and 27.8 percent said they would wait and see, considering price, health concerns and other factors, it said. The remaining 14.8 percent were unsure, said Japan's leading business daily, which polled 60 major restaurants and retailers.
Source: http://news.yahoo.com/s/afp/20060622/hl_afp/japanuspoliticstradehealthmadcow_060622020744;_ylt=AksFYViAxbbrkUblhYYanpOJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA--

[Return to top]

Water Sector

24. *June 22, Journal Star (IL)* — **Farmington must drain water towers.** Farmington, IL, Mayor Bud Stobaugh understands the frustration residents are feeling over a boil order that won't end anytime soon because of a state directive announced Wednesday, June 21. Before the boil order can be lifted, the city's two 75,000−gallon storage tanks and two 150,000−gallon water towers must be drained, cleaned and inspected to find the source of recent bacterial contamination in water samples. Farmington officials learned Wednesday, June 21, of the directive, which came from the Illinois Environmental Protection Agency (IEPA). Stobaugh and City Administrator Roger Woodcock attended a meeting Wednesday in Springfield with IEPA officials, who estimate the draining and cleaning work will take two to four weeks. A routine water sample taken just before Memorial Day weekend tested positive for fecal coliform bacteria. Subsequent samples tested positive for total coliform, which isn't harmful but can indicate the presence of harmful bacteria. That boil order lasted 10 days. Another routine sample taken last week tested positive for total coliform, which led to another boil order.
Source: http://www.pjstar.com/stories/062206/REG_BA63M0FH.025.shtml

25. *June 21, Okeechobee News (FL)* — **South Florida Water Management District holds annual "Hurricane Freddy" exercise.** South Florida Water Management District (SFWMD) emergency management personnel gathered in the auditorium of the Okeechobee service center to hear a conference call that reported storm damages in the 16 counties served by SFWMD. There were reports of missing personnel, power outages, flooding, and requests for additional personnel and pumps. The Okeechobee field office reported flooding around Fisheating Creek and requested pumps. A meteorologist gave the present weather conditions and location of the hurricane and rainfalls in different areas of the state. It was all part of SFWMD's annual "Hurricane Freddy" exercise to test the agency's emergency operations, preparedness and recovery plans. According to the scenario, Hurricane Freddy was the second worse natural disaster to hit the U. S. −− next to Hurricane Katrina. It had hit Tampa, covering it with 18 feet of water. Hurricane Freddy was patterned after an actual 1921 Category 4 hurricane. According to the scenario, the SFWMD headquarters in West Palm Beach had been rendered inoperable by the imaginary storm.
Source: http://www.newszap.com/articles/2006/06/21/fl/lake_okeechobe e/aoke01.txt

[Return to top]

Public Health Sector

26. *June 22, Agence France−Presse* — **Malaysia declares itself free of bird flu.** Malaysia has declared itself free of bird flu, saying there had been no outbreaks of the deadly disease for the past three months, but added it would remain on high alert. "Malaysia is now free of the H5N1 virus after three months since the last infection," Agriculture Minister Muhyiddin Yassin told a press conference on Thursday, June 22. "Our surveillance has shown that there are no outbreaks," he said. "So today we declare Malaysia free of the bird flu virus." However, the minister said that with the disease still spreading in neighboring Indonesia where 39 people have died, bans on imports of birds and eggs from affected countries remained in place and tough action would be taken against smugglers. Malaysia reported a rash of outbreaks of the H5N1 strain from February when it appeared in free−range chickens in villages near the capital Kuala Lumpur, triggering the slaughter of tens of thousands of poultry. Since then the country has suffered five other outbreaks of the virus among poultry in the northern states of Perak and Penang.
Source: http://news.yahoo.com/s/afp/20060622/hl_afp/healthflumalaysiaschedlead_060622105138;_ylt=Ahv8UUOhMY4XJBCKf2F29LuJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

27. *June 22, Reuters* — **Dutch report second Creutzfeldt−Jakob case.** A second Dutch person has been diagnosed with the human variant of mad cow disease after a woman died from the disease last year, Dutch health authorities said on Thursday, June 22. The Dutch Institute for Health and Environment said in a statement that the person most probably got infected by eating contaminated meat products. A 26−year−old Dutch woman, who had been diagnosed with the brain wasting Creutzfeldt−Jakob (vCJD) disease −− the human form of bovine spongiform encephalopathy or mad cow disease −− died in May 2005. Over 150 cases of vCJD have been reported around the world, mostly in Britain, but also in France, Ireland, Italy, Japan, Canada and the U.S.
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006−06−22T124908Z_01_L22218944_RTRUKOC_0_US−DUTCH−MADCOW.xml&archived=False

28. *June 22, New Scientist* — **Early human bird flu death uncovered in China.** A man died of H5N1 flu in Beijing in November 2003 −− two full years before China admitted any human cases of H5N1. The death of the 24−year−old from bird flu came months before China even admitted H5N1 was circulating in its poultry. The man was tested for respiratory illness because of concern in the wake of the Severe Acute Respiratory Syndrome (SARS) epidemic. The case suggests that, as has long been suspected, many more people have caught H5N1 flu in China than have been reported, and for a longer time. "It's a very important issue that needs to be clarified urgently," Roy Wadia, a spokesperson for the World Health Organization, said on Thursday, June 22. "It raises questions as to how many other cases may not have been found at the time or may have been found retrospectively in testing." Wu−Chun Cao of the State Key Laboratory of Pathogens and Biosecurity in Beijing and seven colleagues from four top medical and genomics institutes in Beijing report that in November 2003 a man died in the city four days after being hospitalized for pneumonia and acute respiratory distress. Further tests on samples from his lungs have found H5N1.
Source: http://www.newscientist.com/article/dn9388−early−human−bird−flu−death−uncovered−in−china.html

29. *June 21, Associated Press* — **Bird flu spread among family members.** The World Health Organization (WHO) has concluded that human−to−human transmission likely occurred among seven relatives who developed bird flu in Indonesia. In a report obtained Wednesday, June 21, by The Associated Press, WHO experts said the cluster's index case was probably infected by sick birds and spread the disease to six family members. One of those cases, a boy, then likely infected his father, it said. The WHO stressed the virus has not mutated and that no cases were detected beyond the family. Seven of the eight relatives died last month, but one was buried before samples could be taken to confirm bird flu infection. "Six confirmed H5N1 cases likely acquired (the) H5N1 virus through human−to−human transmission from the index case ... during close prolonged contact with her during the late stages of her illness," the report said. The report was distributed at a closed meeting in Indonesia.
Source: http://www.forbes.com/entrepreneurs/feeds/ap/2006/06/21/ap28 31717.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

30. *June 22, Department of Homeland Security* — **DHS announces completion of TopOff 4 Command Post Exercise.** The Department of Homeland Security (DHS) on Thursday, June 22, announced it has completed the TopOff 4 Command Post Exercise (T4 CPX), a congressionally mandated counterterrorism exercise for top officials. The exercise, which took place from June 19−22, is a multi−faceted effort to prevent and respond to a simulated terrorist attack using weapons of mass destruction. The T4 CPX was conducted in conjunction with the Federal Emergency Management Agency Forward Challenge 2006 exercise and the Federal Bureau of Investigation Marble Challenge 06−02 exercise. The T4 CPX focused on senior officials' abilities to respond to a complex and demanding exercise scenario, in accordance with the National Response Plan and National Incident Management System. More than 4,000 Federal, State, local, and tribal senior officials and managers from 85 organizations participated.
Source: http://www.dhs.gov/dhspublic/display?content=5701

31. *June 21, Associated Press* — **Study: Southern San Andreas Fault overdue for big quake.** New earthquake research confirms the southern end of the San Andreas Fault near Los Angeles is overdue for a Big One. The lower section of the fault has not produced a major earthquake in more than three centuries. The new study, which analyzed 20 years of data and is considered one of the most detailed analyses yet, found that stress has been building since then, and the fault could rupture at any moment. "The southern section of the fault is fully loaded for the next big event," said geophysicist Yuri Fialko of the Scripps Institution of Oceanography in La Jolla. Predicting exactly when that might happen, however, is beyond scientists' ability. The analysis was published in the Thursday, June 22, issue of the journal Nature.
Fialko's study: http://www.nature.com/nature/journal/v441/n7096/pdf/nature04 797.pdf

Source: http://www.signonsandiego.com/news/state/20060621−1004−wst−sanandreasfault.html

32. *June 21, KSBI−TV 52 (OK)* — **Soldiers, first responders test network skills.** Exercise Grecian Firebolt, June 10−23, has been testing the connections between military and civilian response agencies in case disaster strikes. The annual exercise also lets soldiers throughout the United States prove their ability to set up voice, data and video services to units operating from Massachusetts to California. This year, the Federal Emergency Management Agency (FEMA) is using Grecian Firebolt 2006 to test its network and how it communicates with the Army's. "Grecian Firebolt provides an excellent venue for testing equipment interoperability between FEMA and Army communications systems; sharing tactics, techniques, and procedures; contingency planning; design of communications infrastructure; and building habitual interagency relationships," said Maj. Gen. Donna Dacier, commander of the 311th Theater Signal Command.
Source: http://www.ksbitv.com/technology/3066781.html

33. *June 19, Government Computer News* — **Geospatial and flood−mapping operations are helping to streamline emergency response.** While withstanding a storm of criticism for its response to recent large−scale natural disasters, the Federal Emergency Management Agency (FEMA) has continued to make substantial investments in its geospatial and flood−mapping operations. The strategy has provided both a ray of sunshine for the beleaguered agency and a public relations coup, as Web maps and data have proved to be almost ideal mechanisms to reach out to disaster victims en masse and respond to their requests. In the long term, geospatial technology should help FEMA become more effective in its core missions of disaster response and hazard mitigation, officials said. Though some experts say the two terms have become almost synonymous, geospatial technology is generally regarded as going beyond the now−familiar marriage of electronic maps and data of geographic information systems by adding more sophisticated analysis. FEMA’s geospatial analysts work side by side with first responders, either in the field or remotely, helping them make critical decisions and direct resources where they are needed most. FEMA’s other major geospatial effort is a massive, five−year effort begun in November 2004 to update the flood maps provided for communities that are members of the National Flood Insurance Program.
Source: http://www.gcn.com/print/25_16/41081−1.html

[Return to top]

Information Technology and Telecommunications Sector

34. *June 22, IDG News Service* — **Third Microsoft Excel attack posted.** On Tuesday, June 20, a hacker published code that takes advantage of an unpatched flaw in the Microsoft Corp. spreadsheet software, the third such exploit to be disclosed in the past week. This attack could be used to run unauthorized software on a PC, but it requires that the victim first be tricked into opening an Excel document, according to an alert published on the Securitytracker.com Website. The attack takes advantage of Adobe Systems Inc.'s Flash technology, which can be used to provide graphics and animation to Excel documents. "When the target user opens the Excel file, the [malicious] Flash code will execute automatically without user interaction," the alert states.

Security Tracker advisory: http://www.securitytracker.com/alerts/2006/Jun/1016344.html
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001349

35. *June 21, CNET News* — **Yahoo outages frustrate some users.** Outages across the country left some registered Yahoo users without e−mail or instant−messaging capability on Tuesday, June 20, and Wednesday, June 21. While the company acknowledged an early morning outage Wednesday, some Yahoo user reports indicated that services were also out on Tuesday night in some areas. There were also complaints of Yahoo Sports Fantasy Baseball being unavailable. While Yahoo's e−mail and messenger services were inaccessible for some people, Yahoo Search, Yahoo News and the Yahoo home pages seem to have been unaffected. Yahoo did not release any details on the percentage of users affected, or what specifically caused the "software−related issues."
Source: http://news.com.com/Yahoo+outages+frustrate+some+users/2100−1032_3−6086485.html?tag=nefd.top

36. *June 21, SC Magazine* — **Two new World Cup worms appear.** Two new e−mail worms are exploiting interest in the World Cup to attack computers and turn them into part of a botnet. The Sixem−A worm spreads using a variety of disguises, including subject lines such as "Naked World Cup game set," "Soccer fans killed five teens" and "Crazy soccer fans," to try and dupe unsuspecting users into clicking on a malicious attachment. Another worm, W32.Worm.Zade.A, is a new mass e−mailing worm that sends itself out as a World Cup−themed e−mail. It also attempts to take control of the user's computer. Recent research by McAfee found that fans of the Angolan national team are most likely to be targeted by spam and spyware than other soccer fans. Fans of Brazil and Portugal were also highly targeted.
Source: http://www.scmagazine.com/uk/news/article/565447/two+new+world+cup+worms+appear/

37. *June 21, Websense Security Labs* — **Malicious Code Alert: SMS lures for Trojan bot.** Websense Security Labs has received reports of users being lured to install malicious code via Short Message Service (SMS) messages (also known as text messages). Victims receive an SMS message on their mobile phone, thanking them for subscribing to a fictitious dating service. The message states that the subscription fee of $2.00 per day will be automatically charged to their cell phone bill until their subscription is cancelled at the online site. Users who visit the site to unsubscribe from the service are prompted to download a Trojan bot. The site does not attempt to exploit any vulnerabilities; instead, the attacker provides instructions to bypass the Internet Explorer security warning prompt. This bot is Dumador variant and is controlled by the Web−based HTTP controller.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=531

38. *June 21, WTAE−TV (PA)* — **New Trojan attacks governmental and political networks.** Several political groups in the country have begun an assault of governmental and other political groups' computer systems and networks. How it works: A USB port known as the "Thumb Drive" is left lying in an obvious place where it could be found. The idea is that an employee of the target agency will pick up the Thumb Drive and try to identify who the device belongs to by inserting it into a machine inside the building. Once the drive is opened, it will contain files that are given titles that entice the finder of the USB device to open a file. This

Trojan can be the type that will upload personal employee or patient data. Other times the file downloads a virus that is designed to attack the computer and any network it is connected to. Source: http://www.thepittsburghchannel.com/news/9404442/detail.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of active exploitation of a new vulnerability in Microsoft Excel. Successful exploitation could allow an attacker to execute arbitrary code with the privileges of the user running Excel. For more information please the review the following:

Technical Cyber Security Alert: TA06−167A
http://www.us−cert.gov/cas/techalerts/TA06−167A.html

Vulnerability Note: VU#802324 http://www.kb.cert.org/vuls/id/802324

We are continuing to investigate this vulnerability. US−CERT recommends the following actions to help mitigate the security risks:

Install anti−virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

Review the workarounds described in Microsoft Security Advisory 921365:
http://www.microsoft.com/technet/security/advisory/921365.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04−010 for more information on working with email attachments: http://www.us−cert.gov/cas/tips/ST04−010.html

FDIC Phishing Scam

US−CERT continues to receive reports of phishing scams that target online users. Recently, the phishing scam targeted the customers of Federal Deposit Insurance Company (FDIC) insured institutions.

Customers of FDIC institutions received a spoofed email message, which claims that their account is in violation of the Patriot Act, and that FDIC insurance has been

removed from their account until their identity can be verified. The message provides a link to a malicious web site which prompts users to enter their customer account and identification information.

If you were affected by the FDIC phishing scam, please refer to the FDIC Consumer Alert for assistance: http://www.fdic.gov/consumers/consumer/alerts/phishing.html

US−CERT confirms that the federal agencies including Department of Homeland Security (DHS) mentioned in the fraudulent email have not sent out an email that requests customer account or identification information.

US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT:
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to OnGuard Online, a consortium of Federal Agencies: http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution and file a complaint with the Federal Trade Commission (FTC) immediately if you believe your account or financial information has been compromised.
https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03

Review FTC's web site on how to protect yourself from identity theft:
http://www.consumer.gov/idtheft/

Review the OnGuard Online practical tips to guard against Internet fraud, secure your computer, and protect your personal information:
http://onguardonline.gov/phishing.html

Refer to the US−CERT Cyber Security Tip on Avoiding Social Engineering and Phishing Attacks: http://www.us−cert.gov/cas/tips/ST04−014.html

Refer to the CERT Coordination Center document on understanding Spoofed/Forged Email: http://www.cert.org/tech_tips/email_spoofing.html

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing

incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 26777 (−−−), 6881 (bittorrent), 38566 (−−−), 445 (microsoft−ds), 33947 (−−−), 25 (smtp), 24232 (−−−), 32790 (−−−), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

39. *June 22, Washington Post* — **Dike may not hold Lake Okeechobee in a big hurricane.** Engineers hired by a Florida state agency are reporting that weaknesses in the vast dike around the lake again pose a "grave and imminent danger to the people and the environment of South Florida." If the dike fails, the flow from the lake could submerge vast areas, threaten water supplies in much of South Florida and cause tens of billions of dollars in damage, according to the report, ordered by the South Florida Water Management District. Every year, according to engineers, the dike has a one in six chance of failing. The warning has come as a shock in a place where residents had long believed that the rebuilt dike, about 25 feet high, encircling the lake would protect them from a catastrophe. Commissioner Warren Newell, who represents Palm Beach County on a board covering the lake area, said, "Now we're running around trying to get evacuation plans in place, mobilize equipment, and find shelters for thousands of people." About 40,000 people live around Lake Okeechobee, one of the nation's largest freshwater lakes.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/20/AR2006062001270.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer